Securing DevOps: Where to start and what to measure

Stefania Chaplin @devstefops
Solutions Architect @ Gitlab

Credit to Image Creators
Agenda

- #whoami
- What?
- Who?
- How?
- Why?
- Summary
- Q&A

Quiz
#whoami

Python, Java
Rest APIs

DevSecOps
AppSec, CloudSec

GitLab

The DevOps Platform

@devstefops
www.devstefops.com

stefania-chaplin
What?
Quiz
What Is DevSecOps?
DevSecOps stands for development, security, and operations.

It's an approach to culture, automation, and platform design that integrates security as a shared responsibility throughout the entire IT lifecycle.
Web

A10. Server - Side Request Forgery
A09. Security Logging and Monitoring Failures
A08. Software and Data Integrity Failures
A07. Identification and Authentication Failures
A06. Vulnerable and Outdated Configurations
A05. Security Misconfiguration
A04. Insecure Design
A03. Injection
A02. Cryptographic Failures
A01. Broken Access Control

OWASP TOP 10 2021
Relative cost to fix bugs, based on time of detection

- Requirements / Architecture
- Coding
- Integration / Component Testing
- System / Acceptance Testing
- Production / Post-release
Common Pain Points

- Security is the bad guy 😈
- Vulnerabilities (known + unknown) make it to production 🚨
- Delays, fails, or.... ‘worse’ 📈
Who?
What is the difference between project mindset vs product mindset?
Fast Secure Stable
## What is Culture?

<table>
<thead>
<tr>
<th>Pathological</th>
<th>Bureaucratic</th>
<th>Generative</th>
<th>Warstrum 2004</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power-oriented</td>
<td>Rule-oriented</td>
<td>Performance-oriented</td>
<td></td>
</tr>
<tr>
<td>Low cooperation</td>
<td>Modest cooperation</td>
<td>High cooperation</td>
<td></td>
</tr>
<tr>
<td>Messengers shot</td>
<td>Messengers neglected</td>
<td>Messengers trained</td>
<td></td>
</tr>
<tr>
<td>Responsibilities shirked</td>
<td>Narrow responsibilities</td>
<td>Risks are shared</td>
<td></td>
</tr>
<tr>
<td>Bridging discouraged</td>
<td>Bridging tolerated</td>
<td>Bridging encouraged</td>
<td></td>
</tr>
<tr>
<td>Failure leads to scapegoating</td>
<td>Failure leads to justice</td>
<td>Failure leads to inquiry</td>
<td></td>
</tr>
<tr>
<td>Novelty crushed</td>
<td>Novelty leads to problems</td>
<td>Novelty implemented</td>
<td></td>
</tr>
</tbody>
</table>

@devstefops www.devstefops.com stefania-chaplin
UNSTABLE
How?
Quiz

Where do we start Securing DevOps?
Some useful reading

🧠 Education
🎨 Secure by Design
🚀 Automation
Developers or Video Gamers?

Age distribution

- Under 18: 0.0%
- 18-34: 30.8%
- 35-44: 21.9%
- 45-54: 17.8%
- 55-64: 13.3%
- 65+: 6.9%
- 70+: 3.7%
- 80+: 2.2%
- 90+: 1.2%
- 100+: 0.9%

Under 18: 24%
18-34: 30%
35-44: 13%
45-54: 12%
55-64: 9%
65+: 6%
Make Security Fun & Easy 😄
Make Security Fun & Easy 🦇
Shift Security Left 🗝️👉

@devstefops

www.devstefops.com

stefania-chaplin
Your Friendly Neighbourhood OWASP

OWASP
Zed Attack Proxy

CycloneDX

OWASP
Dependency-Check

@devstefops
www.devstefops.com
stefania-chaplin
Quiz

How do we measure DevSecOps?
DORA Metrics 🚀⚖

1. LEAD TIME
   Lead time is the time it takes to go from a customer making a request to the request being satisfied. Shorter lead times enable faster feedback.

2. DEPLOYMENT FREQUENCY
   Deployment frequency is a proxy metric for batch size; the more frequently you deploy the smaller the size of the batch. Small batch sizes reduce cycle times, reduce risk and overhead, improve efficiency, increase motivation and urgency, and reduce costs and schedule growth.

3. MEAN TIME TO RESTORE
   Reliability is traditionally measured as time between failures, but in a modern software organization failure is inevitable. Thus, reliability is measured by how long it takes to restore service when a failure occurs.

4. CHANGE FAIL PERCENTAGE
   This metric looks at the percentage of changes made to production that fail; the same as percent complete and accurate in Lean product delivery.

THE SCIENCE OF DEVOPS
ACCELERATE
Building and Scaling High Performing Technology Organizations

Nicole Forsgren, PhD
Jez Humble and Gene Kim

@devstefops
www.devstefops.com

stefania-chaplin
‘Elite performers spend 50% less time remediating security issues than low performers’
Value Stream Analytics

Key metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lead Time</td>
<td>4.5 days</td>
</tr>
<tr>
<td>Cycle Time</td>
<td>2.1 days</td>
</tr>
<tr>
<td>New Issues</td>
<td>3168</td>
</tr>
<tr>
<td>Commits</td>
<td>3950</td>
</tr>
<tr>
<td>Deploys</td>
<td>212</td>
</tr>
</tbody>
</table>

DORA metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment frequency</td>
<td>7.1 per day</td>
</tr>
<tr>
<td>Lead time for changes</td>
<td>0.4 days</td>
</tr>
<tr>
<td>Time to restore service</td>
<td>0.1 days</td>
</tr>
<tr>
<td>Change failure rate</td>
<td>2.0%</td>
</tr>
</tbody>
</table>

Total time

Graph showing average time to completion from Feb 21, 2022 to Mar 21, 2022.
# Beyond Dora Metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
<th>Associated Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>Amount of uptime/downtime in a given time period, in accordance with the service-level agreement</td>
<td>Availability and performance management; network management</td>
</tr>
<tr>
<td>Customer issue volume</td>
<td>Number of issues reported by customers in a given time period</td>
<td>Overarching</td>
</tr>
<tr>
<td>Customer issue resolution time</td>
<td>Mean time to resolve a customer-reported issue</td>
<td>Overarching</td>
</tr>
<tr>
<td>Time to value</td>
<td>Time between a feature request (user story creation) and realization of business value from that feature</td>
<td>Overarching; ATO processes</td>
</tr>
<tr>
<td>Time to ATO</td>
<td>Time between the beginning of Sprint 0 to achieving an ATO</td>
<td>Overarching; ATO processes</td>
</tr>
<tr>
<td>Time to patch vulnerabilities</td>
<td>Time between identification of a vulnerability in the platform or application and successful production deployment of a patch</td>
<td>ATO processes</td>
</tr>
</tbody>
</table>

[https://insights.sei.cmu.edu/blog/the-current-state-of-devsecops-metrics/](https://insights.sei.cmu.edu/blog/the-current-state-of-devsecops-metrics/)
Why?
Why DevSecOps?

- Incorporating security into DevOps helps speed up iterations, we can innovate faster than competitors 🚀
- Vulnerabilities are identified earlier which helps to avoid cyber-attacks 💥
- It helps improve communication and collaboration between teams 🤝

Summary

- Take a #securityfirst approach 🧠
- Break down silos, we are all on the same team! 🌍
- Make it fun, automate & measure results #empowerdevelopers ⚡
Thank you!

stefania@devstefops.com